PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-207360
(43)Date of publication of application : 07.08.1998

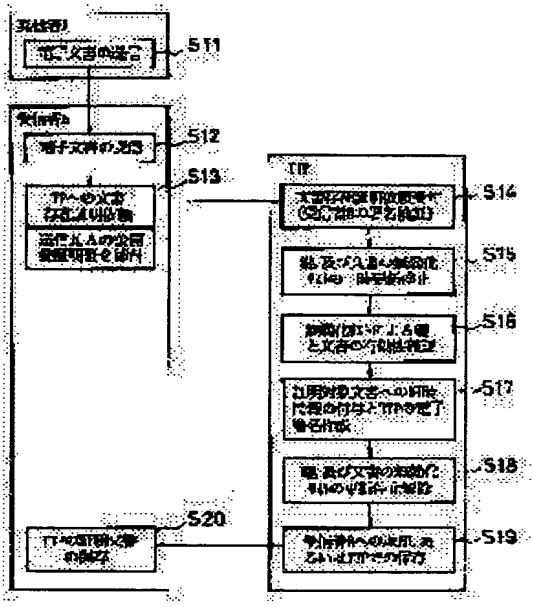
(51)Int.Cl. G09C 1/00
G06F 13/00
G06F 19/00
H04L 9/08
H04L 9/32

(21)Application number : 09-011267
(22)Date of filing : 24.01.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NAKAO MASAYOSHI

(54) EXISTENCE PROVING METHOD FOR ELECTRONIC DOCUMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an existence proving method for electronic document with which the existence proof of already invalidized document is prevented from being erroneously applied by confirming the validity of document.
SOLUTION: A recipient B prepares an existence proof request statement to the third person organization (TTP), applies an electronic signature, adds the public key certificate of transmission source of this document and transmits it to the TTP (step S13), and the TTP verifies the signature of request statement (step S14), temporarily stops updating the invalidizing list of key and document (step S15), confirms the key and document do not exist on the invalidizing list (step S16), applies date/time information to the proof object document, prepares the electronic signature of TTP (step S17), cancels the stop in the update of the invalidizing list of key and document (step S18) and returns it to the recipient B or preserves it at the TTP itself (step S19) so that the existence proof of document can be performed.



LEGAL STATUS

[Date of request for examination] 23.10.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－207360

(43)公開日　平成10年(1998)８月７日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ
	19/00			15/22	Ｎ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｚ
	9/32				６７５Ｂ

審査請求　未請求　請求項の数１　ＯＬ　（全７頁）

(21)出願番号　特願平9－11267

(22)出願日　平成９年(1997)１月24日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　中尾　昌善
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

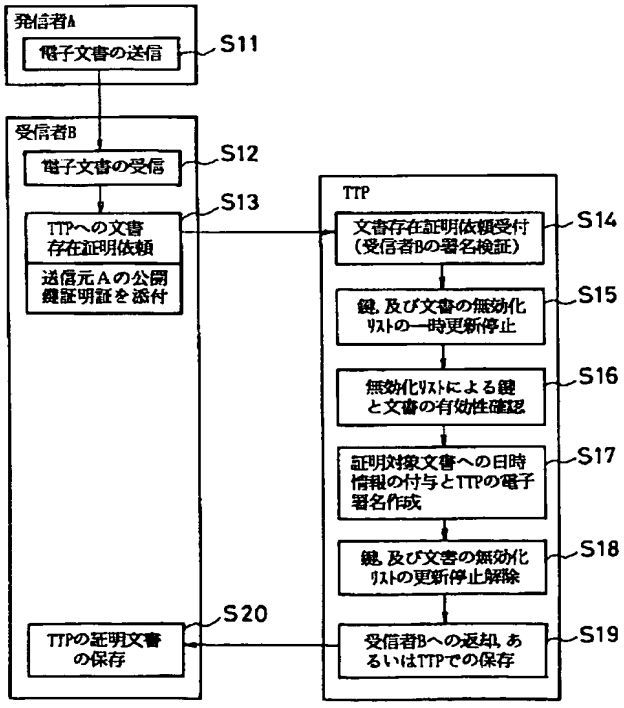
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　電子文書の存在証明方法

(57)【要約】

【課題】　文書の有効性を確認することにより、既に無効化されている文書の存在証明を間違って与えてしまうことがない電子文書の存在証明方法を提供する。

【解決手段】　受信者ＢはＴＴＰ（第三者機関）への存在証明依頼申請書を作成し、電子署名を付与するとともに該文書の送信元の公開鍵証明証を添付して、ＴＴＰに送信し（ステップＳ１３）、ＴＴＰは依頼申請書の署名検証を行い（ステップＳ１４）、鍵および文書の無効化リストの更新を一時停止し（ステップＳ１５）、鍵と文書が無効化リストに存在していないことを確認し（ステップＳ１６）、証明対象文書に日時情報を付与し、ＴＴＰの電子署名を作成し（ステップＳ１７）、鍵と文書の無効化リストの更新停止を解除し（ステップＳ１８）、受信者Ｂに返却またはＴＴＰで保存し（ステップＳ１９）、文書の存在証明を行う。



【特許請求の範囲】

【請求項１】　コンピュータネットワーク上での電子文書の送受信において送信者が受信者に対して送信した電子文書が受信者においてある時点で確かに存在したことを証明する電子文書の存在証明方法であって、

受信者は、存在証明対象の文書の存在証明依頼申請書を作成し、この作成した申請書に電子署名を付与するとともに該文書の送信元の公開鍵証明証を添付して、信頼のおける第三者機関に送信し、

第三者機関は、前記依頼申請書を受け付けると、該依頼申請書の署名検証を行い、公開鍵の認証機関が提供する鍵の無効化リストの更新および第三者機関が提供する文書の無効化リストの更新を一時停止し、前記鍵と文書が無効化リストに存在していないことを確認し、前記文書の存在証明を行うことを特徴とする電子文書の存在証明方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワーク上でＥＤＩ（電子データ交換）やＥＣ（電子商取引）を実現するために必要となる電子文書の送受信において該電子文書がある時点で確かに存在していたことを証明する電子文書の存在証明方法に関する。なお、電子文書とは、一般文書だけに限らず、伝票や契約書類、金銭データ、ドキュメントなどを電子データ化したもの、すなわちコンピュータシステムが扱える形式のディジタルデータにしたものを指すものとする。

【０００２】

【従来の技術】まず、電子文書の存在証明が必要になる背景について説明する。前提として、送信者Ａが受信者Ｂに対して電子文書を送信する場合を考える。一般に、送受信する電子文書が重要なものである時、その文書の作成者が確かに送信者Ａであること、および受信者Ｂが受領した文書には改ざんがなされていないことを保証する必要がある。これに対応する方式として、公開鍵暗号方式による署名通信がある。更に、公開鍵の認証機関ＣＡ（Certification Authority）により発行された公開鍵証明証をその通信に利用することによって、公開鍵の正当性を確かなものにする方式が一般的である。これらの方式は広く知られているため、以下では図５を用いて概略のみを説明する。

【０００３】　送信者Ａは秘密鍵と公開鍵の対を作成する。秘密鍵はそれを作成した本人のみが知っており、一方公開鍵は広く公開されて、誰でも入手して使用可能なものである。秘密鍵と公開鍵には、公開鍵から秘密鍵を容易に作成することはできないという関係が成り立っている。

【０００４】　ＣＡは公開鍵の認証機関であり、主に以下の機能を有している。

（ａ）本人性を確認した上で公開鍵を登録し、それに対してＣＡ署名を付与した公開鍵証明証を発行する機能

（ｂ）登録された公開鍵証明証を希望者に対して配布する機能

（ｃ）登録された公開鍵を無効化し、それを無効化リストに掲載して公表する機能

送信者Ａは、このＣＡに自分の公開鍵を登録することによって、その持ち主であることの証明（公開鍵証明証）を入手する。

【０００５】　送信者Ａは電子文書を作成し、それに対して自分の秘密鍵で署名をつけて、前述の公開鍵証明証とともに受信者Ｂに送信する。ここで、署名を付けるとは、一般に電子文書をハッシュ化し、それを秘密鍵で暗号化することをいう。出来上がったものを、電子署名と呼ぶ。

【０００６】　受信者Ｂは、受信した電子文書と電子署名に対して、送信者Ａの公開鍵（公開鍵証明証から取得）で署名検証する。署名検証とは、送信された電子署名が一緒に送られた電子文書を元にして作成されたものであるか否かを判定することである。この判定の方法は暗号アルゴリズムによって異なる。

【０００７】受信者Ｂにおける署名検証では、　、　の関係により、文書の作成者が公開鍵に対応する秘密鍵を唯一使用可能な送信者Ａ以外に存在しないことを知ることができる。また、電子署名が一緒に送られてきた電子文書を元に作成されたものであるかを判定できるので、途中で改ざんがなされていないことを確認できる。

【０００８】上述したような手続きで送信者Ａが受信者Ｂに電子文書を送信した後、送信者Ａが何らかの理由により、ＣＡに依頼して署名鍵を無効化してしまう場合が想定される。そこでは、次のような問題が発生する。

【０００９】（１）本来の鍵の無効化は、署名鍵が危険にさらされるため、第三者による悪用を防止するために、以後の有効性を停止する目的で使用するものである。しかし、その鍵で署名したすべての電子文書の無効化につながってしまうため、過去に正当にやり取りした文書の有効性も損なわれてしまうことになる。特に、送信者Ａにとって都合が悪い文書に対して、悪意を持って無効化を行う危険が存在する。

【００１０】（２）文書送信側の一方的な都合で鍵の無効化が成立してしまうため、受信側が不利益を受ける可能性がある。

【００１１】このような問題に対する受信側の防御策として有効なのが、文書存在証明である。これは、第三者に対して受信した電子文書を送信し、その第三者が日時情報を付加して管理することにより、ある時点で受信者Ｂが特定の文書を持っていたことを保証する方法である。この文書存在証明という考え方、すなわち第三者が文書の存在を証明すること、および日時情報を付与するということは、世の中の制度として公証役場が存在することからも明らかなように、公知の事実として捉えるこ

とができる。

【００１２】以上で述べたように、電子文書の送受信においては、電子文書の存在証明の仕組みが不可欠であり、その考え方は一般的なものということができる。しかし、それを実現する手段については、いくつかの方法が考えられ、本発明もその方法の一部を構成するものである。いくつか考えられる方法の一つとして、ＴＴＰ（Trusted Third Party ：信頼できる第三者機関）が文書存在証明を行う場合が想定できる。これは、単なる第三者機関ではなく、公に信頼できるという条件が与えられた機関が提供する点に特徴がある。このＴＴＰが提供する文書存在証明の仕組みは、一般的に図６に示すような方法となる。

【００１３】図６に示すＴＴＰによる従来の文書存在証明方法について説明する。送信者Ａが電子文書を受信者Ｂに対して送信する（ステップＳ６１）。受信者Ｂは、この電子文書を受信すると（ステップＳ６３）、ＴＴＰへの文書存在証明依頼を行う（ステップＳ６５）。なお、この時、受信者Ｂは、対象となる文書に自分の電子署名と公開鍵証明証を添付して送信する。

【００１４】ＴＴＰは、受信者Ｂからの文書存在証明依頼を受信すると、受信者Ｂの署名検証を行うことにより、確かに受信者Ｂからの依頼であることを確認する（ステップＳ６７）。それから、ＴＴＰは、受け取った電子文書に日時情報を付加し、それにＴＴＰの電子署名を作成付与する（ステップＳ６９）。ＴＴＰは、この日時情報を付加した電子文書を受信者Ｂに返却するかまたはＴＴＰ内で保存する（ステップＳ７１）。この保存した文書が後で文書存在証明を行う証拠品となる。

【００１５】ＴＴＰから日時情報を付加された電子文書が受信者Ｂに返却された場合には、受信者Ｂはこの返却されてきた証明情報を保存する（ステップＳ７３）。

【００１６】

【発明が解決しようとする課題】上述したように、ＴＴＰによる従来の文書存在証明方法では、受信者Ｂから送信されてきた文書存在証明対象の文書が既に無効なものである場合にも、信頼できるはずのＴＴＰが文書存在証明を与えてしまうという問題がある。なお、文書が無効な場合とは、送信者Ａの署名鍵が無効化されている場合と、ＴＴＰを介した文書の無効化処理がなされている場合（特願平９－８８７３号参照）とがある。

【００１７】本発明は、上記に鑑みてなされたもので、その目的とするところは、文書の有効性を確認することにより、既に無効化されている文書の存在証明を間違って与えてしまうことがない電子文書の存在証明方法を提供することにある。

【００１８】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、コンピュータネットワーク上での電子文書の送受信において送信者が受信者に対して送信した電子文書が受信者においてある時点で確かに存在したことを証明する電子文書の存在証明方法であって、受信者は、存在証明対象の文書の存在証明依頼申請書を作成し、この作成した申請書に電子署名を付与するとともに該文書の送信元の公開鍵証明証を添付して、信頼のおける第三者機関に送信し、第三者機関は、前記依頼申請書を受け付けると、該依頼申請書の署名検証を行い、公開鍵の認証機関が提供する鍵の無効化リストの更新および第三者機関が提供する文書の無効化リストの更新を一時停止し、前記鍵と文書が無効化リストに存在していないことを確認し、前記文書の存在証明を行うことを要旨とする。

【００１９】請求項１記載の本発明にあっては、受信者は存在証明依頼申請書を作成し、電子署名を付与するとともに該文書の送信元の公開鍵証明証を添付して、第三者機関に送信し、第三者機関は依頼申請書の署名検証を行い、確かに受信者からの依頼であることを確認し、鍵および文書の無効化リストの更新を一時停止し、鍵と文書の有効な状態を文書存在証明が完了するまで保持し、第三者機関が鍵の有効性を確認してから文書存在証明を成立させるまでの期間に鍵の無効化がなされてしまう不都合を防止し、鍵と文書が無効化リストに存在していないことを確認し、文書の存在証明を行う。

【００２０】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００２１】図１は、本発明の一実施形態に係る電子文書の存在証明方法の処理手順を示すフローチャートである。本実施形態の電子文書の存在証明方法は、コンピュータネットワーク上での電子文書の送受信において文書の受信者Ｂから信頼できる第三者機関（以下、ＴＴＰ（Trusted Third Party ）と略称する）に文書存在証明を依頼する際に、文書送信元である送信者Ａの公開鍵証明証を添付し、ＴＴＰで送信元の署名鍵の有効性と当該文書の有効性を確認するものであり、この場合に公開鍵の認証機関（以下、ＣＡ（Certification Authority ）と略称する）の提供する鍵の無効化とＴＴＰが提供する文書の無効化を一時的に停止することにより、鍵および文書の有効性を正しく確認可能としている。このために、本実施形態は、鍵の無効化リスト更新一時停止機能、文書無効化リスト更新一時停止機能、鍵と文書の有効性確認機能を有する。

【００２２】まず、図１を参照して、本実施形態の電子文書の存在証明方法の処理手順について説明する。送信者Ａが受信者Ｂに文書を送信し（ステップＳ１１）、受信者Ｂは該電子文書を受信する（ステップＳ１２）。該受信者Ｂは、ＴＴＰに文書存在証明を依頼する（ステップＳ１３）。この場合、受信者Ｂは対象となる申請書に送信者Ａの公開鍵証明証を添付する。

【００２３】ＴＴＰは、受信者Ｂからの文書存在証明依

頼を受け付けると、受信者Ｂの署名検証を行い、確かに受信者Ｂからの依頼であることを確認する（ステップＳ１４）。また、ＴＴＰは、ＣＡが提供する鍵の無効化リスト更新一時停止機能とＴＴＰが提供する文書無効化リスト更新一時停止機能を用いて、鍵と文書の無効化リストの更新を一時停止し、鍵と文書の有効な状態を文書存在証明が完了するまで保持するようにする（ステップＳ１５）。これにより、ＴＴＰが鍵の有効性を確認してから文書存在証明を成立させるまでの期間に鍵の無効化がなされてしまう不都合を防止することが可能となる。

【００２４】それから、ＴＴＰは、鍵と文書の有効性確認機能を用いて、鍵と文書が無効化リストに掲載されていないことを確認する（ステップＳ１６）。また、ＴＴＰは、受け取った証明対象の電子文書に日時情報を付加するとともに、該情報のＴＴＰの電子署名を作成して付与する（ステップＳ１７）。このステップＳ１７が、存在照明が成立したときとなる。次に、ＴＴＰは、ステップＳ１５で行った鍵および文書の無効化リストの更新の一時停止を解除し（ステップＳ１８）、ステップＳ１７で作成した文書存在証明情報およびその電子署名を受信者Ｂに返却するかまたはＴＴＰ内に保存する（ステップＳ１９）。受信者ＢはＴＴＰから返却されたＴＴＰ証明文書を保存する（ステップＳ２０）。

【００２５】上述したように、本実施形態では、文書存在証明対象となった文書の有効性を確認した上での文書存在証明が可能となり、ＴＴＰの信頼性を向上させることができる。

【００２６】次に、図２および図３に示すフローチャートを参照して、更に詳細な作用について説明する。

【００２７】送信者Ａは、通信処理機能３１ａを使用して電子文書を受信者Ｂに対して送信し（ステップＳ３１）、受信者Ｂは該電子文書を通信処理機能３２ａにより受信する（ステップＳ３２）。なお、送信者Ａと受信者Ｂとの間には一般的な公開鍵暗号方式を用いた電子署名通信が行われているものであり、前記電子文書に電子署名および公開鍵証明証が付与されている。

【００２８】該受信者Ｂは、電子文書を受信すると、電子文書作成／編集機能３３ａにより文書存在証明依頼申請書を作成する（ステップＳ３３）。この場合、文書存在証明依頼申請書には証明の対象となる電子文書と送信者Ａの公開鍵証明証が添付される。受信者Ｂは、文書存在証明依頼申請書を作成すると、通信処理機能３４ａを用いてＴＴＰに送信する（ステップＳ３４）。この受信者ＢとＴＴＰとの間の通信にも同様に一般的な公開鍵暗号方式を用いた電子署名通信が使用されているものである。

【００２９】ＴＴＰは、通信処理機能３５ａを用いて受信者Ｂからの文書存在証明依頼を受信すると（ステップＳ３５）、署名検証機能３６ａを用いて受信者Ｂの署名検証を行い、確かに受信者Ｂからの依頼であることを確認する（ステップＳ３６）。それから、ＴＴＰは、鍵の無効化リスト更新一時停止手段３７ａを用いて、ＣＡが提供する鍵の無効化リストの更新を一時停止し（ステップＳ３７）、またＴＴＰは、文書無効化リスト更新一時停止手段３８ａを用いて、ＴＴＰが提供する文書の無効化リストの更新を一時停止し（ステップＳ３８）、鍵と文書の有効な状態を文書存在証明が完了するまで保持する。これにより、ＴＴＰが鍵の有効性を確認してから文書存在証明を成立させるまでの期間に鍵の無効化がなされてしまう不都合を防止することが可能となる。

【００３０】次に、ＴＴＰは、鍵と文書の有効性確認手段３９ａを用いて、ＣＡが提供する鍵の無効化リストを確認し（ステップＳ３９）、更に文書の無効化リストを確認し（ステップＳ４０）、これにより鍵と文書が無効化リストに掲載されていないことを確認する。そして、ＴＴＰは、日時取得機能およびデータ編集機能４１ａを用いて、受信者Ｂから受け取った証明対象の電子文書に日時情報を付与し、該情報のＴＴＰの電子署名を署名生成機能４２ａにより作成して付与する（ステップＳ４２）。

【００３１】それから、ＴＴＰは、鍵の無効化リスト更新一時停止解除手段４３ａを用いて、前記ステップＳ３７で行った鍵の無効化リストの更新の一時停止を解除し（ステップＳ４３）、更に文書無効化リスト更新一時停止解除手段４４ａを用いて文書の無効化リストの更新の一時停止を解除する（ステップＳ４４）。また、ファイル入出力機能４５ａを用いて文書存在証明情報を保存し（ステップＳ４５）、通信処理機能４６ａを用いて文書存在証明情報を受信者Ｂに送信する（ステップＳ４６）。

【００３２】次に、図４を参照して、上述した鍵の無効化リスト更新一時停止手段３７ａの構成について説明するとともに、また文書無効化リスト更新一時停止手段３８ａ、鍵と文書の有効性確認手段３９ａについても説明する。

【００３３】鍵の無効化リスト更新一時停止手段３７ａは、図４に示すように、更新一時停止機能５１、その解除機能５２、および無効化要求機能５３から構成されている。また、該無効化リスト更新一時停止手段は更新可否情報と無効化リストを与えられている。更新可否情報は０が更新可能であり、１が更新不可である。更新一時停止機能５１と解除機能５２は更新可否情報の書換えを行う。無効化要求機能５３は更新可否情報を見て、無効化リストの更新可否を制御する。文書無効化リスト更新一時停止手段３８ａの構成も図４に示すものとほぼ同じである。

【００３４】また、鍵と文書の有効性確認手段３９ａによる鍵の有効性確認処理は、受信者Ｂから入手した送信者Ａの公開鍵証明証を元に、ＣＡが提供する無効化リストの参照手段を用いて実施することができる。文書の有

効性確認処理は、ＴＴＰが文書の無効化手段を提供しており、無効化手段のハッシュ値が保存されていることを前提として、文書存在証明対象になった文書に対してもハッシュ値を計算し、両者を比較することにより当該文書が無効化対象になっていないか確認することができる。なお、ハッシュ値を用いたのは、ディジタルデータの同一性確認の容易性を考慮したものであり、ハッシュ化することが必須ではない。

【００３５】

【発明の効果】以上説明したように、本発明によれば、受信者は存在証明依頼申請書を作成し、電子署名を付与するとともに該文書の送信元の公開鍵証明証を添付して、第三者機関に送信し、第三者機関は依頼申請書の署名検証を行い、確かに受信者からの依頼であることを確認し、鍵および文書の無効化リストの更新を一時停止し、鍵と文書が無効化リストに存在していないことを確認し、文書の存在証明を行うので、送信者からの文書の有効性を確認してから文書存在証明を行うことができ、文書存在証明を成立させるまでの期間に鍵の無効化がなされてしまう不都合も防止し、第三者機関の信頼性を向上することができるとともに、コンピュータネットワーク上での信頼のおける電子文書の送受信を実現することが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る電子文書の存在証明方法の処理手順を示すフローチャートである。

【図２】図１に示す電子文書の存在証明方法の更に詳細な処理手順を示すフローチャートの一部である。

【図３】図１に示す電子文書の存在証明方法の更に詳細な処理手順を示すフローチャートの一部であり、図２のフローチャートに続く部分である。

【図４】図２，３の処理手順で使用されている鍵の無効化リスト更新一時停止手段の構成を示す図である。

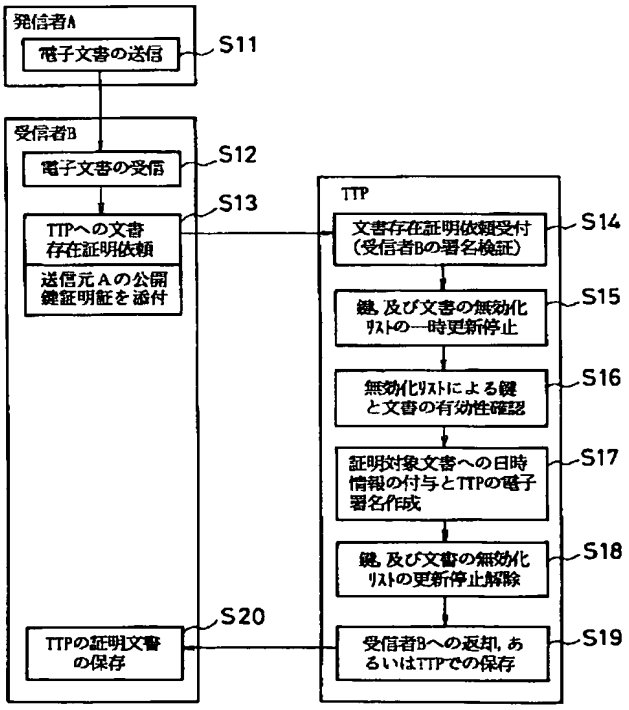
【図５】文書存在証明方法を議論する前提となる公開鍵暗号方式による従来の電子文書署名通信の概要を示す図である。

【図６】ＴＴＰによる従来の文書存在証明方法の処理手順を示すフローチャートである。

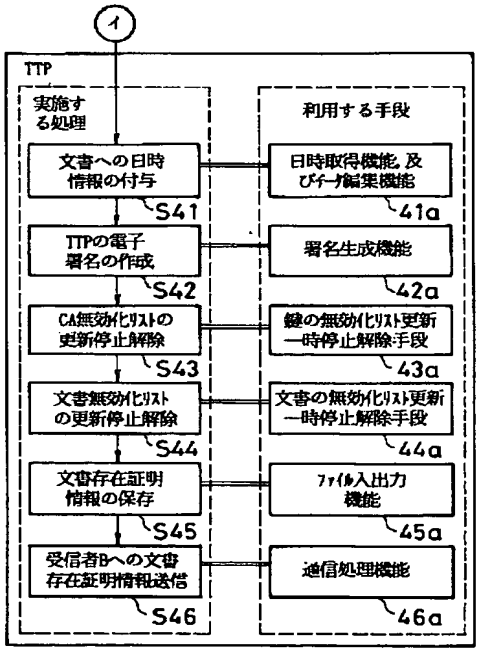
【符号の説明】

３７ａ　鍵の無効化リスト更新一時停止手段
３８ａ　文書の無効化リスト更新一時停止手段
３９ａ　鍵の文書の有効性確認手段
４３ａ　鍵の無効化リスト更新一時停止解除手段
４４ａ　文書の無効化リスト更新一時停止解除手段

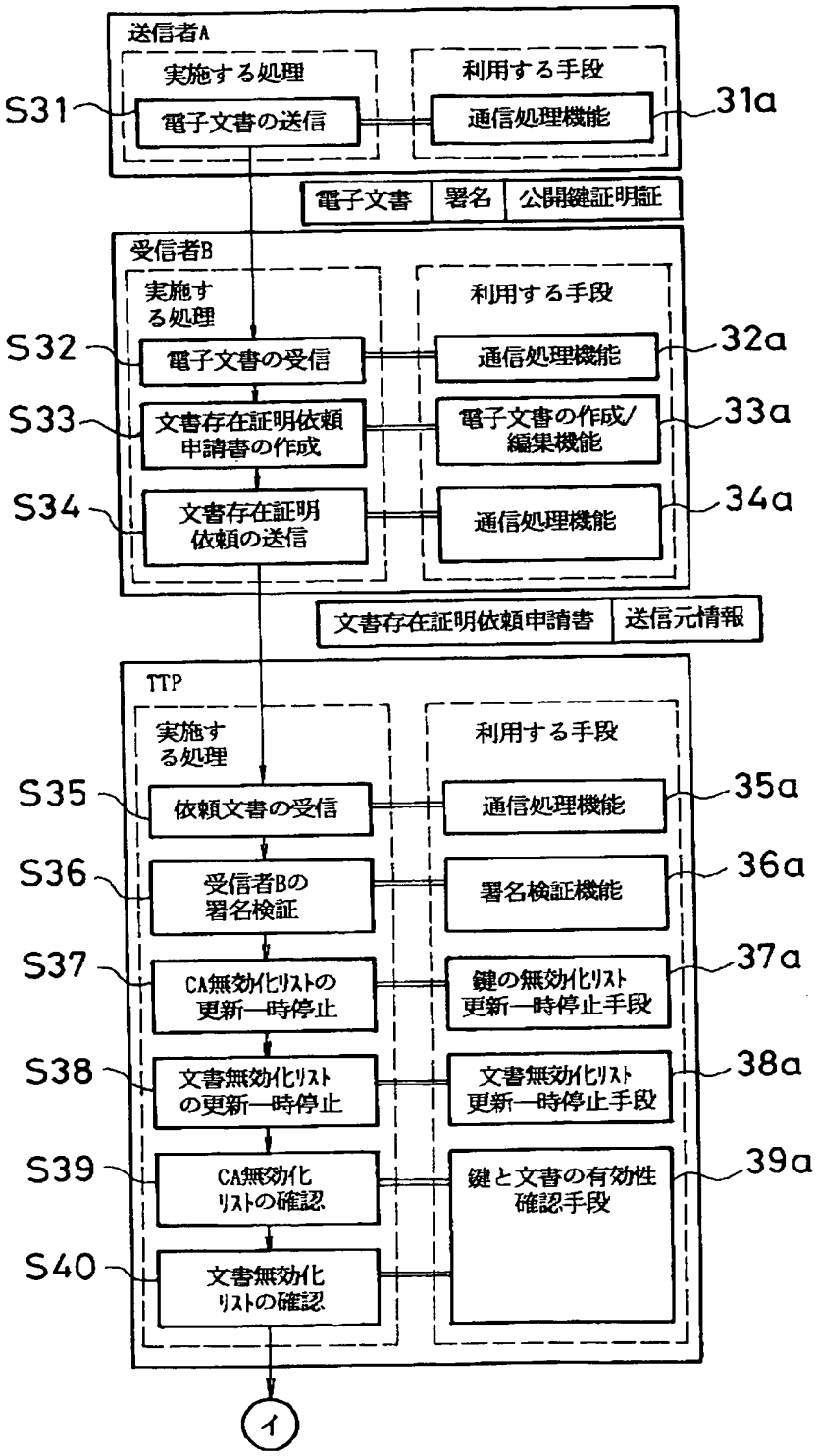
【図１】



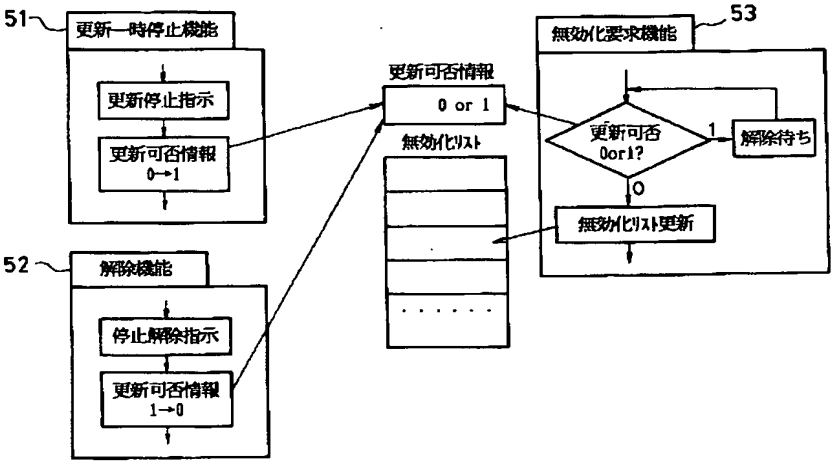
【図３】



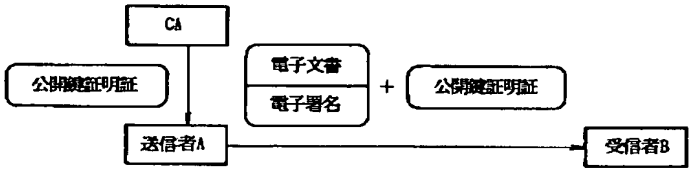
【図２】


送信者A
実施する処理
利用する手段
S31
電子文書の送信
通信処理機能
31a
電子文書
署名
公開鍵証明証
受信者B
実施する処理
利用する手段
S32
電子文書の受信
通信処理機能
32a
S33
文書存在証明依頼申請書の作成
電子文書の作成/編集機能
33a
S34
文書存在証明依頼の送信
通信処理機能
34a
文書存在証明依頼申請書
送信元情報
TTP
実施する処理
利用する手段
S35
依頼文書の受信
通信処理機能
35a
S36
受信者Bの署名検証
署名検証機能
36a
S37
CA無効化リストの更新一時停止
鍵の無効化リスト更新一時停止手段
37a
S38
文書無効化リストの更新一時停止
文書無効化リスト更新一時停止手段
38a
S39
CA無効化リストの確認
鍵と文書の有効性確認手段
39a
S40
文書無効化リストの確認
イ

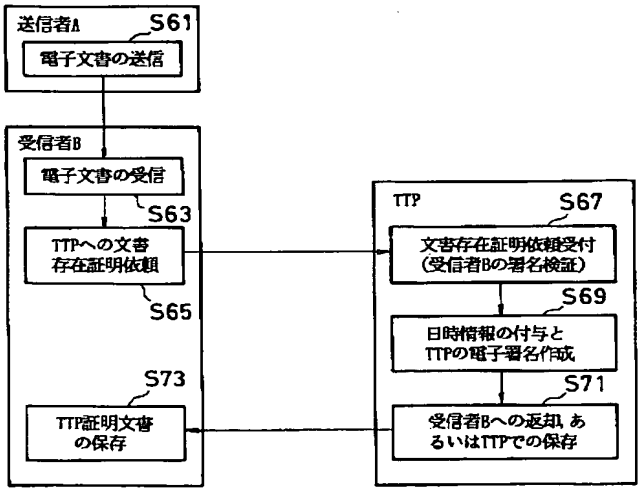
【図４】


51
更新一時停止機能
更新停止指示
更新可否情報
0→1
52
解除機能
停止解除指示
更新可否情報
1→0
更新可否情報
0 or 1
無効化リスト
53
無効化要求機能
更新可否
0or1?
1
解除待ち
0
無効化リスト更新

【図５】


CA
公開鍵証明証
電子文書
電子署名
+
公開鍵証明証
送信者A
受信者B

【図６】


送信者A
S61
電子文書の送信
受信者B
電子文書の受信
S63
TTPへの文書
存在証明依頼
S65
S73
TTP証明文書
の保存
TTP
S67
文書存在証明依頼受付
(受信者Bの署名検証)
S69
日時情報の付与と
TTPの電子署名作成
S71
受信者Bへの返却 あ
るいはTTPでの保存